1. (Currently Amended) A method for authenticating a user over a network, comprising the steps of:

providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network;

confirming the identity of the user to the central server, using the identification box;

sending a unique math table from the central server to the identification box, with the unique math table being stored at both the central server and the identification box;

measuring a first biometric parameter from the user with the biometric reader, and storing the first biometric parameter in encrypted form at the identification box and at the central server;

sending a user request for authentication from the identification box to the central server;

~~a)~~ sending a random number from ~~a remote site~~ the central server to ~~a local site~~ the identification box ~~of a user,~~;

~~b)~~ measuring a ~~first~~ second biometric parameter from ~~said~~ the user with ~~a~~ the biometric reader~~,~~;

encrypting the second biometric parameter;

~~c)~~ comparing, at the identification box, ~~said first~~ the second encrypted biometric parameter with ~~a~~ the ~~previously~~ previously-stored ~~second~~ first encrypted biometric parameter~~,~~;

~~d)~~ operating on ~~said~~ the random number, at the identification box, with ~~a~~ the unique math table to create a first cryptogram when a positive match occurs between ~~said~~ the first and second encrypted biometric parameters;

operating on the random number, at the central server, with the unique math table to create a second cryptogram;~~,~~

~~e)~~ sending ~~said~~ the first cryptogram from the identification box ~~said local site~~ to ~~said remote site~~ the central server;

~~for comparison~~ comparing, at the central server, the first cryptogram with ~~a~~ the second cryptogram ~~n internally generated cryptogram.~~; and

confirming the authenticity of the user when a positive match occurs between the first cryptogram and the second cryptogram.

2. (Cancelled) A method for authenticating a user over a network as in claim 1 further comprising the step of encrypting said first biometric parameter to form a first encrypted biometric parameter.

3. (Cancelled) A method for authenticating a user over a network as in claim 1 further comprising the step of generating a first cryptogram from said random number if said first encrypted biometric parameter positively matches said second encrypted biometric parameter.

4. (Cancelled) A method for authenticating a user over a network as in claim 1 further comprising the step of sending said first generated cryptogram to said remote site for comparison with a second cryptogram.

5. (Cancelled) A method for authenticating a user over a network as in claim 4 wherein said second cryptogram is generated from a site other that from said local site.

6. (Currently Amended) A method for authenticating a user over a network as in claim 1 further comprising the step of

allowing the user access to a second remote site if ~~said~~ the first cryptogram matches ~~said~~ the second cryptogram.

7. (Currently Amended) A method for authenticating a user over a network comprising the steps of:

providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network;

confirming the identity of the user to the central server, using the identification box;

sending a unique math table from the central server to the identification box, with the unique math table being stored at both the central server and the identification box;

measuring a first biometric parameter from the user with the biometric reader, and storing the first biometric parameter in encrypted form at the identification box and at the central server;

sending a user request for authentication from the identification box to the central server;

~~a)~~ sending a first random number from the central server ~~a remote site~~ to the identification box ~~the site of the user~~;~~,~~

~~b)~~ measuring a second biometric parameter from ~~said~~ the user with ~~a~~ the biometric reader;

encrypting the second biometric parameter;~~,~~

~~c)~~ comparing, at the identification box, the second encrypted ~~said first encrypted~~ biometric parameter with ~~a second encrypted biometric parameter~~ the previously-stored first ~~on said~~ encrypted biometric ~~reader~~ parameter;~~,~~

~~d)~~ generating, at the identification box, a second random number when ~~said~~ the first encrypted biometric parameter does not positively match ~~said~~ the second encrypted biometric parameter;~~,~~

~~e)~~ operating on ~~said~~ the second random number, at the identification box, with ~~a~~ the unique math table to create a first cryptogram when a positive match fails to occur between said first and second encrypted biometric parameters,

operating on the first random number, at the central server, with the unique math table to create a second cryptogram;

~~f)~~ sending ~~said~~ the first cryptogram from ~~said local site~~ the identification box to ~~said remote site for~~ the central server;

~~comparison~~ comparing, at the central server, the first cryptogram with ~~an internally generated~~ the second cryptogram; and

denying the authenticity of the user when there is no match occurs between the first cryptogram and the second cryptogram.~~.~~

8. (Currently Amended) A method for authenticating a user over a network as in claim 7 ~~furhter~~ further comprising the step of denying the user access to a second remote site if ~~said~~ the first cryptogram does not match ~~said~~ the second cryptogram.

9. (Cancelled) A method for authenticating a user over a network as in claim 7 further comprising the step of generating a first cryptogram from said second random when said first encrypted biometric parameter does not match said second biometric parameter.

10. (New) A method according to claim 1 further comprising:

providing a second identification box at a second remote site, with the second identification box including a second biometric reader, and with the second identification box and the central server being connected over the network;

sending a user request for authentication from the second identification box to the central server;

sending the unique math table and the first encrypted biometric parameter from the central server to the second identification box;

sending a second random number from the central server to the second identification box;

measuring a third biometric parameter from the user with the second biometric reader;

encrypting the third biometric parameter;

comparing, at the second identification box, the third encrypted biometric parameter with the first encrypted biometric parameter;

operating on the second random number, at the second identification box, with the unique math table to create a third cryptogram when a positive match occurs between the first and third encrypted biometric parameters;

operating on the second random number, at the central server, with the unique math table to create a fourth cryptogram;

sending the third cryptogram from the second identification box to the central server;

comparing, at the central server, the third cryptogram with the fourth cryptogram; and

confirming the authenticity of the user when a positive match occurs between the third cryptogram and the fourth cryptogram.

11. (New) A system for authenticating a user over a network, comprising:

an identification box at the local site of the user, with the identification box including a biometric reader, and the identification box being connected to a central server over the network;

the identification box comprising apparatus adapted to:

(i) receive a unique math table from the central server and to store the same;

(ii) measure a first biometric parameter from the user and store the first biometric parameter in encrypted form;

(iii) send a user request for authentication to the central server;

(iv) receive a random number from the central server;

(v) measure a second biometric parameter from the user;

(vi) encrypt the second biometric parameter;

(vii) compare the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter;

(viii) operate on the random number with the unique math table to create a first cryptogram when a positive match occurs between the first and second encrypted biometric parameters; and

(ix) send the first cryptogram to the central server.